AKAMAI THREAT ADVISORY

2016 State of the Dark Web

Author: Benjamin Brown
Akamai SIRT

Akamai
FASTER FORWARD

1.0 / Overview / 2016 was an active year for the dark web. New cryptocurrencies found use alongside Bitcoin (BTC), and the general offerings of the dark web markets shifted significantly. Several high-profile hacker forums and underground marketplaces have disappeared, with new ones popping up to take their place. Interesting and new darknet-based privacy services were announced in the forms of an ISP and a VPN offering. Additionally, 2016 saw impactful policy and enforcement efforts targeting the dark web and its users. These State-backed efforts continue to be a major topic of discussion in dark web user and market forums, driving individuals to share analysis of takedowns, potential impacts of new policy, operational security (OPSEC) tutorials and advice, personal and secondhand accounts of interactions with law enforcement, and suggestions for how best to guard particular dark web services and their users from future enforcement efforts by the State.

2.0 / Deep Web vs. Dark Web vs. Darknet / Deep web, Dark web, Darknet — while these terms may be used interchangeably by the media, they represent distinct, but related segments of the Internet. The deep web refers to pages and services on servers that are accessible through standard Internet browsers and methods of connection, but not indexed by major search engines. Often the deep web is not indexed by search engines because of website or service misconfiguration, search listing opt-out requests, paywalls, registration requirements, or other content access limitations. The dark web, a relatively small portion of the deep web, relates to web services and pages that are intentionally hidden. These services and pages cannot be directly accessed through standard browsers alone, they rely on the use of an overlay network requiring specific access rights, proxy configurations, or dedicated software. Darknets are frameworks where access is restricted at the network level, for example Tor or I2P. Private VPNs and mesh networks also fall into this category. Network traffic over these frameworks is masked in such a way that snooping shows only which darknet you are connected to and how much data you move, without necessarily revealing what sites you visit or the content of said data. This is in contrast with simply interacting with the clearnet or unencrypted surface and deep web services, in which case your ISP and network operators between you and your requested resources can openly see the content of the traffic you generate.

3.0 / Different Darknets / Tor is not the only darknet framework out there. While it is the most popular, there are a number of increasingly popular "anonymity networks" to be aware of. None of these should be expected to offer any anonymity from a dedicated adversary: they are research projects in the ergonomics of anonymous communication. Almost as old as the Tor project, is the Invisible Internet Project (I2P). I2P, like Tor, is a network that sits on top of the Internet and provides some masking of its user's identities. However, to claim that I2P makes its users fully anonymous would be misleading at best. Most commonly implemented using Java, the open-source I2P protocol currently supports Web surfing, chatting, blogging, and file sharing. Released in March of 2000, Freenet is probably the most well known darknet after Tor and I2P. A peer-to-peer (P2P) platform that aims to be censorship and surveillance resistant, Freenet suffers from a relatively small number of nodes, making it potentially easier to unmask targeted individuals, especially if an actor has the drive and resources to run a significant number of their own nodes, which is suspected to have happened with the "Black Ice Project"[1]. This is an aspect of the framework the Freenet developers and user community are working to make more resilient.

Zeronet is another such framework, but it is based on BTC cryptography and the BitTorrent network. Much like Freenet, Zeronet aims to be a decentralized P2P network that resists orders to be taken down or otherwise knocked offline. Python-based and open source, the project allows users to access specific "ZeroNet URLs" through regular browsers with the option for users to mask their IP addresses. Another P2P mesh network in development is Netsukuku. Unlike Tor, Netsukuku isn't another overlay network. Netsukuku is a separate physical network and dynamic routing system capable of handling up to 2^32 nodes without the need for centralized servers. Riffle, an MIT project, is being reported as potentially faster than Tor, providing stronger security guarantees, and boasting a "bandwidth and computation efficient communication system with strong anonymity"[2,3,4,5]. We believe it is worth following the development of these darknet technologies, their potential adaptations, and their future adopters to better understand how they are being used. This knowledge will then help us realize how darknet technologies may impact our customers.

4.0/ Tor Project Shakeups / In December 2015, the former Executive Director and President of the Electronic Frontier Foundation (EFF), Shari Steele, was brought on as the Tor Project's new director. In May 2016, Jacob Applebaum resigned from the Tor Project, and an entirely new board of directors was appointed. Additionally, the group's headquarters moved from Cambridge, MA to Seattle, WA[6]. In response to this large shake-up, one of the project's oldest and largest contributors, Lucky Green, also walked away from Tor., Lucky Green reportedly took the critical Bridge Authority node, 'Tonga', and several fast Tor relays with him. In a June 2016 article by the Pew Research Center titled, "The State of Privacy in Post-Snowden America," the authors state that their research found that, "some 86% of internet users have taken steps online to remove or mask their digital footprints, but many say they would like to do more or are unaware of tools they could use." The report goes on to explain that "some 74% say it is 'very important' to them that they be in control of who can get information about them, and 65% say it is 'very important' to them to control what information is collected about them."[7] With sentiments like these, we expect that we'll continue to see a rise in usership of privacy oriented services such as Tor.

5.0 / Tor Marketplace Shifts / On April 13, 2016, one of the largest dark web markets, Nucleus Market, disappeared. Many suspect that this was an exit scam. An exit scam occurs when marketplace owners wait until a sufficiently large amount of BTC has been shifted into the marketplace, then close the site to block outgoing transfers, and make off with the BTC they have locked into the site. The top dark web markets list has since been shaken up. The top five in terms of size and traffic are now:

- AlphaBay
- Dream Market
- Hansa Market
- Valhalla (formerly Silkkitie — Finnish for Silk Road)
- Outlaw Market (one of the oldest)

The owner of Sheep Marketplace has perpetrated what is arguably the largest dark web scam to date. Tomáš Jiřikovský absconded with about 40 million dollars worth of marketplace users' bitcoin. He is currently in Moravian police custody and faces up to 12 years in prison for the theft of bitcoins and enabling a drug trade[8].

In July of 2016, TheRealDeal market, known for selling software exploits, 0-days, and breached data dumps (such as Tumblr, LinkedIn, MySpace, and various Healthcare providers) had their main admin seemingly vanish without a trace. Surprisingly, vendors and sellers could still move their bitcoin in and out for quite some time, could still engage in transactions, and no bitcoins in escrow appeared to be missing. However, since the end of October 2016, the URL for the market has remained unreachable. There is no credible explanation in sight and it remains unclear what actually happened.

6. 0 / Underground Economy Trends on Tor Markets / 2015, and more notably 2016, saw a major shift in dark web market offerings, from a focus on illicit drugs to one of financial fraud. These offerings include malware, compromised credential databases, personally identifiable information (PII), medical records, financial services accounts, hacking tutorials, credit card numbers, and a glut of compromised digital accounts for a wide range of services. Single and bulk compromised account logins are readily available across the top five dark web markets and prices are falling as more become available. Accounts on Yahoo, Dropbox, Walmart, Gamestop, Uber, Amazon, Ebay, Netflix, and many more currently average about a dollar per account. Much of this is fueled by the rise of account checker activity and cybercriminal moves from disparate forums to new dark web marketplaces.

7. 0 / Hacker Forum Whack-a-Mole / As of January 2016, darknet hacking forum "Hell" is back on the scene with a new head admin. "Hell" gained attention after leaking the Adult Friend Finder breach, and the site shut down in July 2015. The site's head admin Ping, briefly disappeared and returned a few days later, causing much confusion and even more suspicion[9]. In December 2016, the infamous Darkode forum, allegedly frequented by LizardSquad members, also reappeared after being shuttered by the Feds under Operation Shrouded Horizon in 2015[10]. The new version of Darkode has shifted back to a clearnet address, following a failed relaunch on the Tor network. These, along with the recently hacked Nulled forum, were hotbeds for inexperienced hackers (aka script kiddies) actively trading tutorials, tools, exploits, hacked data, and DDoS and hacking services for hire. In each case of resurrection, the forum's rosters have majorly shifted. With these shifts, it will be interesting to see where the members continue to make their new homes. Traditionally, hacker forums have been targets in a giant game of whack-a-mole, by both law enforcement and competing forums.

8.0 / New Dark Web ISPs and VPNs / In July 2016, at the Hackers on Planet Earth conference (HOPE), Gareth Llewelyn announced the creation of Brass Horn Communications, a new ISP that utilizes the OnionDSL system to Torrify all client traffic at the router, moves it through the ISP controlled bridge, and performs a series of Tor hops before engaging in browsing activities. This system purportedly prevents the ISP from capturing client traffic logs meaningful for identification, calling itself "Surveillance Frustrating Broadband"[11]. This system is still in beta. However, if it gains market traction, Surveillance Frustrating Broadband could make end-user and traffic origin identification interesting for controls that rely on IP blacklisting and geoblocking.

In a similar vein, a new VPN service has emerged called TGVPN (formerly I2VPN). This VPN service claims to leverage Tor (or I2P as an option) and BTC technologies to increase anonymity and privacy. A BTC address and signature are used to authenticate to the VPN while the user traffic is tunneled through three levels of encryption. User traffic is encrypted first by OpenVPN, then by WrapVPN, and then by TLS. The developers claim not to use

OpenVPN's cryptography deeming it unsafe. Instead, they employ custom cryptography using primitives X25519 (Elliptic-curve Diffie-Hellman over Curve25519), XSalsa20, and Poly1305. The code is open-source and available via their GitHub[12]. The developers also claim to /dev/null all logs and boast a warrant canary[13].

9.0 / Cryptocurrency Movement /

9.1 / Bitcoin / 2016 was a great year for Bitcoin (BTC), beating out Brazil's Real (BRL) currency to become the best performing currency of the year. BTC more than doubled its value and gained 126% on the year. The price drive was due, in large part, to two main factors. These factors include the relative volatility and devaluation of a number of fiat currencies, and action on the Chinese markets[14]. In the second half of 2016, the Yuan accounted for 98% of all BTC trading. Looking at value volatility data from 2011 to 2017, it is clear that BTC stability has been steadily increasing.

What does all this mean for the dark web? With relative stability, easy transferability, and an increase in value, we will likely continue to see BTC as a premier currency used by cyber criminals, privacy advocates, and those intrigued by the concept of alt-currencies or cryptocurrencies. From 2015 to 2016, BTC has already taken huge swaths of territory from the likes of Perfect Money, WebMoney, Payza, and OKpay (note: For now, Eastern European actors in cybercrime forums and Russian-language Tor marketplaces tend to defy this trend and hold tight to these alternate payment frameworks).

9.2 / Monero / In August 2016, both AlphaBay and Oasis dark web markets announced that they would begin supporting Monero as a payment source. Over the next month, Monero saw a 669% increase in value. In 2016, Monero's market capitalization exploded from $5M USD to $185M USD. Additionally, Monero was integrated into the economy of Massive Multiplayer Online Role-Playing Game CryptoKingdom and is accepted at an increasing number of dark web and clearnet gambling consortiums.

Monero, unlike bitcoin, does not use a public transaction ledger and claims to support completely anonymous transactions. Based on an adaptation of the CryptoNote protocol, using one-time ring signatures and stealth addresses, this implementation claims to render the blockchain opaque. Additionally, developers are currently working on I2P integration to hide any IP addresses involved in transactions. Given the privacy claims, we should expect to start seeing this payment structure used for anything from stolen data or exploit transactions to DDoS or data shakedown schemes.

9.3 / Zcash / Zcash, another privacy-oriented cryptocurrency, had its speculation-hounded debut in 2016. In October, it was sitting on an outrageous valuation of $2M USD, though the following months saw a tumble. Valuation dipped below $100 USD by the end of November. Early 2017 has seen Zcash continuing to decline in value, with a dip below $40 USD. Unlike BTC and Monero, Zcash isn't seeing a lot of investor interest going into 2017.

Utilizing the zk-SNARK, Zero Knowledge proof allows the Zcash blockchain to verify transactions without revealing sensitive data about the transaction's participants. While this is a new framework, that does not yet have a proven track record, the Zcash project's CEO is Zooko Wilcox-O'Hearn. Wilcox-O'Hearn is a security specialist known for his work on the Tahoe Least-Authority File Store (Tahoe-LAFS). Additionally, he is a member of the development teams for both the ZRTP protocol and the BLAKE2 cryptographic hash function. Rumblings on the dark web market forums indicate that Zcash may very well join Monero as an alternative to BTC in 2017.

10.0 / Dark Web Leveraged for Attacks / Throughout 2016, Akamai continued to see the use of the Tor network to obfuscate malicious traffic using tools such as SQLmap, Tor's Hammer, UFONet, HIVE, and newer versions of LOIC (Low-Orbit Ion Cannon). It is important to note that the malicious traffic seen from Tor nodes has not been volumetrically significant[15]. Akamai keeps an up-to-date list of Tor exit nodes that customers can use when blocking traffic; however, this does carry the risk of dropping legitimate customer traffic over Tor. Due to bandwidth limitations, DDoS attacks over Tor are less concerning than SQL Injection (SQLi) and Remote Code Execution (RCE) type attacks. For SQLi and RCE attacks a well tuned Web Application Firewall (WAF) would be of more use for allowing legitimate traffic to filter through while actively blocking malicious traffic.

11.0 / Legal and Law Enforcement Action / George Cottrell, is an aide to Nigel Farage who is a prominent member of Britain's U.K. Independence Party. Goerge was nabbed by the FBI on 21 charges related to dark web money laundering, fraud, blackmail and extortion[16]. Arrests of dark web market sellers continued, with the takedown of the Italian Mafia Brussels gang[17] ,which was known for prolific MDMA peddling. Irishmen Kyle Hall, Richard Sinclair, and Stephen Rodgers were all arrested for dealing MDMA, in addition to other drugs[18]. Abudullah Almashwali and Chaudhry Ahmad Farooq were indicted for large-scale cocaine and heroin vending on the Alphabay dark web marketplace[19]. Furthermore, IcyEagle was caught selling identity fraud related services, including hijacked bank accounts and extensive PII packets. Michael Andrew Ryan of Kansas was also apprehended for selling handguns through dark web markets[20].

In response to the July 2016 mass shooting in Munich, where the gunman had procured his weapon through the dark web, the head of the German BKA (Federal Police) Holger Muench announced a new focus on dark web movements affecting the country[21]. This new push culminated in the August 11 joint operation between the Federal Customs Administration and Germany's Central Office of Cybercrime. At that time, six Bavarian properties were searched, netting four suspects, 11 kilograms of amphetamine, 150 grams of cocaine, 250 grams of heroin, 175 grams of MDMA, 1,425 ecstasy pills, 645 grams of marijuana, an indoor growing operation with 72 marijuana plants, and a BTC wallet containing close to $400,000 worth of BTC[22].

Austria expressed similar concerns to those of Germany, and passed an amendment to the country's Weapons Act. This amendment grants law enforcement the authority to carry firearms privately and off-duty. Additionally, this amendment greatly increased penalties for unauthorized possession or unauthorized transmission of firearms. Austria's Ministry of the Interior expects these changes to be effective advances for battling dark web based weapons trafficking[23]. Real-world policy and enforcement is shifting in direct response to the dark web.

A prolific counterfeiting organization was taken down in a large operation headed by Europol. The criminal team of eight, known as "NapoliGroup," was involved in investment scams, distributing more than 7,600,000 Euros worth of counterfeit notes. NapoliGroup used both the dark web and BTC extensively[24].

Above and beyond all these examples, is the case of the U.S. FBI hacking of suspects around the world. According to October 2016 evidentiary hearing court transcripts, at least 8,000 computers in 120 countries were exploited under a single warrant[25,26]. This was part of operation PlayPen, in which the FBI took control of a dark web child pornography website, using a number of network and browser exploitation techniques to expose end users[27].

12.0 / 2017 AND BEYOND / A big shift is expected in 2017 and 2018, with dark web markets moving to all-in-one privacy-oriented social platforms. The developers of cryptocurrency, ShadowCash, are reportedly building their own privacy platform, which they have named UMBRA. UMBRA boasts a Slack-like end-to-end encrypted chat function, cryptocurrency wallet management, secure payment and balance transfer mechanisms, and a P2P marketplace. The developers are also working on Tor and I2P integration to further bolster user privacy[28].

Another such framework in development is the Komodo platform. This platform aims to protect user anonymity through the aforementioned Zcash zero knowledge proofs and a blockchain that uses a delayed Proof of Work mechanism (dPoW). The platform also includes a multi-wallet called Iguana for storing funds in different cryptocurrencies. EasyDEX is their decentralized cryptocurrency exchange system. And for transactions involving 'real-world' assets and fiat currency Komodo uses the Pegged Asset Exchange (PAX) boasting support for the anonymous exchange of 32 fiat currencies using the Komodo coin (KMD) framework[29].

Platforms like these focus on hardening the most common vectors of digital privacy compromise currently experienced within dark web marketplace exchanges. While they don't solve any problems related to trucking in and shipping tangible goods, these platforms provide the underground marketplaces of tomorrow with good incentives. These incentives attract vendors and customers who are looking for greater ease-of-use and a stronger sense of security.

References

1. http://www.grandforksherald.com/news/crime-and-courts/3885134-child-predators-use-technology-law-enforcement-does-too
2. http://news.mit.edu/2016/stay-anonymous-online-0711
3. https://techcrunch.com/2016/07/11/mits-anonymous-online-communications-protocol-riffle-could-beat-tor-at-its-own-game/
4. http://www.theregister.co.uk/2016/07/13/riffle_next_gen_anonymity/
5. https://people.csail.mit.edu/devadas/pubs/riffle.pdf
6. https://www.nytimes.com/2016/07/28/technology/tor-project-jacob-appelbaum.html
7. http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/
8. http://archiv.ihned.cz/c1-63752430-jak-se-praly-bitcoiny-miliony-z-ciziny-vila-napsana-na-dedecka
9. https://motherboard.vice.com/read/back-from-hell-hacking-site-founder-resurfaces-after-going-missing
10. https://motherboard.vice.com/read/darkode-brand-relaunches
11. https://brasshorncommunications.uk/
12. https://github.com/ZenifiedFromI2P/wrapvpn
13. http://i2vpn.i2p
14. http://www.forbes.com/sites/laurashin/2017/01/09/bitcoins-price-was-volatile-last-week-but-not-last-year/#4aac30954247
15. https://www.akamai.com/us/en/about/news/press/2015-press/akamai-releases-second-quarter-2015-state-of-the-internet-security-report.jsp
16. http://www.bbc.com/news/uk-politics-38495175
17. http://deredactie.be/cm/vrtnieuws.english/News/1.2693360
18. http://www.belfasttelegraph.co.uk/news/northern-ireland/men-accused-of-running-major-drugs-operations-on-dark-web-34957444.html
19. https://www.justice.gov/usao-edca/pr/two-brooklyn-men-indicted-distributing-heroin-and-cocaine-dark-web-marketplace-alphabay
20. https://www.justice.gov/usao-ndga/pr/icyeagle-dark-web-vendor-stolen-information-charged-atlanta

21. http://www.reuters.com/article/us-germany-cyber-idUSKCN1071KW
22. http://www.focus.de/regional/rheinland-pfalz/limburgerhof-polizei-schlag-gegen-drogenhandel-im-darknet-festnahme-von-4-verdaechtigen-und-durchsuchungen_id_5825124.html
23. https://www.parlament.gv.at/PAKT/PR/JAHR_2016/PK1344/
24. http://www.lostrillone.tv/castellammare-trafficavano-soldi-falsi-in-mezza-europa-8-arresti/11500.html
25. https://www.documentcloud.org/documents/3224249-Hearing-in-Tippens-Day-1.html
26. https://www.documentcloud.org/documents/3224250-Hearing-in-Tippens-Day2.html
27. https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-beco-11e5-83d4-42e3bceea902_story.html
28. https://umbra.shadowproject.io/
29. https://komodoplatform.com